INITIAL STATEMENT OF REASONS:

This action will adopt administrative provisions governing inmate access to computers and electronic data processing equipment. These provisions have regulatory effect but are not yet adopted as regulations.

Due to the advancement of computer technology and the increase in the utilization of computers by businesses and the general public, these provisions were necessarily established to interpret and make specific Penal Code Section 502, as amended by Chapter 1357 of the Statutes of 1989, and Penal Code Section 2702, as added by Chapter 1357 of the Statutes of 1989, and to ensure the security of the computer data and computer systems of the Department of Corrections as well as those of the public.

The Department must determine that no alternative considered would be more effective in carrying out the purpose of this action or would be more effective and less burdensome to affected private persons than the action proposed.

New Subsection 3040(g) is adopted to prohibit inmates who have a history of computer fraud or abuse from being given work or educational assignments whereby they may gain access to a computer This is necessary to guard the integrity of the data in the Department’s database and to keep departmental personnel records and inmate information from being accessed or tampered with. These provisions are necessarily established to interpret and make specific Penal Code Section 2702.

Existing subsection 3040(g) is relocated to subsection (h).

New Section 3041.3 is adopted to protect the data of the Department and to protect the public from tampering, corruption, damage, and unauthorized access to lawfully created computer systems, and is necessary to interpret and make specific Penal Code Section 502.

New subsection 3041.3(a) is adopted to protect computer data as stated above, without being so prohibitive as to prevent the use of computers in vocational or educational programs, or in the repair or use of computers as part of an inmate work program.

New subsection 3041.3(b) is adopted to prevent inmates from accessing other databases or corrupting existing data or computer systems. This will decrease the potential for new crimes to be perpetrated from within the facilities.

New subsection 3041.3(c) is adopted to restrict program development by inmates and to closely scrutinize the use of inmates as programmers, as well as to secure the computers used by inmates, the data utilized by the inmates, and the documents produced by the inmates. These provisions were necessarily established to interpret and make specific Penal Code Section 502.

New subsection 3041.3(d) is adopted to control and label the area where inmates may access computers. This is necessary to prevent inadvertent access to computers that have not been secured.

New subsection 3041.3(e) is adopted to prevent inmates from accessing computers that may contain personnel records, inmate information, or any information that may be of a sensitive nature.

New subsection 3041.3(f) is adopted to prevent inmates from assigning a password to their PC. This is necessary to ensure that CDC staff will be able to review and inspect inmates' documents and data.

New subsection 3041.3(g) is adopted to prevent inmates from having diskettes or other storage media in their possession. This is necessary to prevent the transference of unauthorized documents/data and also to prevent the spreading of computer viruses that could disrupt departmental or public computer systems or corrupt departmental or public databases.

New subsection 3041.3(h) is adopted to prohibit inmates from possessing computers as part of their personal property. This is necessary to prevent security breaches as previously discussed.

New subsection 3041.3(i) is adopted to prevent the introduction of a computer virus that could corrupt the Department's computer system and database, or computer systems and databases of the public.

New subsection 3041.3(j) is adopted to prohibit inmates who have a history of computer fraud or abuse from gaining access to a computer This is necessary to guard the integrity of the data in the Department's database and to keep departmental personnel records and inmate information from being tampered with.

New subsection 3041.3(k) is adopted to prevent the hook-up of a "stand alone" computer to telephone lines, thus enabling connection to a local area network (LAN). This will prevent inmates from accessing other databases and potentially corrupting existing data and will inhibit the potential of new crimes being perpetrated from within the facilities.

New subsection 3041.3(l) is adopted to prevent inmates from getting into the "background" of the Department's computer system and will prevent the corruption or the Department's databases.

New subsection 3041.3(m) is adopted to allow inmates to refurbish computers as part the Computers for Schools Program, which allows the donation of computers refurbished by prison inmates to elementary schools. The unclothed body search which is to be conducted prior to exiting the work area is necessary to prevent the confiscation of machine parts which may be used as weapons and protects safety and security in the prisons.

New subsection 3370(b) is adopted to allow inmates to view their own case records file in the presence of staff. Maintaining case records in the Department's database is considerably less expensive than maintaining hard-copy files. Inmates must be allowed access to these files.

Existing subsections 3370(b) and (c) are redesignated as subsections (c) and (d).